(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 499 797 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 153(4) EPC

(43) Date of publication:
19.06.2019 Bulletin 2019/25

(21) Application number: **16916105.6**

(22) Date of filing: **16.11.2016**

(51) Int Cl.:
H04L 12/24 *(2006.01)*

(86) International application number:
PCT/CN2016/106057

(87) International publication number:
WO 2018/049725 (22.03.2018 Gazette 2018/12)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA MD

(30) Priority: **14.09.2016 CN 201610825161**

(71) Applicant: **Wangsu Science & Technology Co., Ltd.**
Shanghai 200030 (CN)

(72) Inventors:
- **LI, Tengchao**
  Shanghai 200030 (CN)
- **LIU, Xiaopeng**
  Shanghai 200030 (CN)

(74) Representative: **Hanna Moore + Curley**
Garryard House
25/26 Earlsfort Terrace
Dublin 2, D02 PX51 (IE)

(54) PPTP VPN-BASED ACCELERATED ACCESS METHOD, APPARATUS AND DEVICE

(57) The present disclosure provides a method, apparatus, and device for PPTP VPN based access acceleration. A PPTP VPN system includes a client-side, a first server, a VPN server, and a second server cluster supporting a GRE protocol connected between the first server and the VPN server. When the client-side starts an accelerated access, the first server receives a first PPTP message and a first GRE message from a same client-side, and encapsulates the first GRE message. An encapsulated first GRE message and the first PPTP message are send to a same second server. The first GRE message is encapsulated and the source addresses of the first GRE message and the first PPTP message are changed. Therefore, the reliability of the transmission can be achieved. Reverse transmission is no difference. The present disclosure accelerates the access speed of the VPN server and improves the access quality of the user.

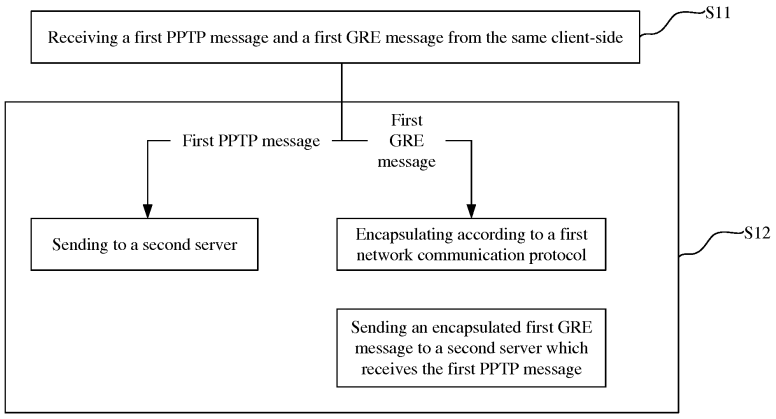

FIG. 4

EP 3 499 797 A1

Description

FIELD OF THE DISCLOSURE

[0001] The present disclosure generally relates to network security technology and, more particularly, to a method, apparatus, and device for PPTP VPN based access acceleration.

BACKGROUND

[0002] PPTP (Point to Point Tunneling Protocol) is a network technology for supporting multiprotocol virtual private network (VPN), which works on a second layer. Based on the PPTP protocol, a remote user can secure access to a corporate network via Microsoft Windows NT Workstation, Windows XP operating system, Windows 2000 operating system, Windows 2003 operating system, Windows7 operating system, and other systems installed with a point-to-point protocol. The remote user can dial into a local ISP, and securely link to the corporate network over the Internet.

[0003] The basic process of tunneling technology is that at an interface between a source LAN and a public network, data (e.g., data from the data link layer or the network layer in the seven-layer ISO/OSI model) as a payload is encapsulated in a data format that can be transmitted over the public network, and at an interface between a destination LAN and the public network, the payload can be taken out by de-encapsulating the data.

[0004] The VPN built by using the PPTP has relatively strong stability and security, and PPTP is also used by relatively mainstream VPN servers nowadays. There are multiple VPN access scenarios using PPTP, for example, employees who travel for work can use the VPN to access the enterprise internal network, and subsidiaries can use the VPN to access the parent enterprise internal network. However, this way of access has cross-regional and cross-carrier factors. The poor access quality and slow access speed make it difficult to meet the need of customer on access quality.

[0005] Currently, a relatively common agent system is shown in FIG. 1. A server 110 is arranged on a client-side router, which intercepts TCP (Transmission Control Protocol) traffic, and/or UDP (User Datagram Protocol) traffic, and the like. The intercepted traffic is forwarded to a nearest B server 120 via a dedicated high-speed network for back-to-the-source. Thereby, the access speed can be greatly enhanced. However, the agent system as shown in FIG. 1 does not support the GRE protocol (Generic Routing Encapsulation). Therefore, the agent system cannot accelerate the PPTP VPN traffic.

SUMMARY

[0006] In view of the above-mentioned drawbacks of the conventional technology, the objectives of the present disclosure is to provide a method, apparatus, and device for PPTP VPN based access acceleration to solve the problem that PPTP VPN based transparent agent system does not support the GRE protocol and cannot accelerate the PPTP VPN traffic.

[0007] To achieve the above-mentioned objectives and other related objectives, the present disclosure provides a method for PPTP VPN based access acceleration, wherein a PPTP VPN system includes a client-side, a first server, a VPN server, and a second server cluster supporting a GRE protocol connected between the first server and the VPN server, and the second sever cluster is an acceleration system. The method for PPTP VPN based access acceleration comprises:receiving a first PPTP message and a first GRE message from a same client-side; for the first PPTP message, sending the first PPTP message to the second server; and for the first GRE message, encapsulating the first GRE message based on a first network communication protocol and sending the encapsulated first GRE message to the second server receiving the first PPTP message.

[0008] According to an embodiment of the present disclosure, the first network communication protocol is a network communication protocol that supports the transmission of data packets between the first server and a second server in the process of network communication.

[0009] According to an embodiment of the present disclosure, the first sever is connected with the client-side or the first server is a virtual server arranged on the client-side.

[0010] According to an embodiment of the present disclosure, IP(Internet Protocol)addresses of the client-side are extracted from the first PPTP message and the first GRE message, respectively; a Hash calculation is performed on the IP address of the client-side extracted from the first PPTP message to obtain an IP address of the second server, and according to the IP address of the second server obtained from the Hash calculation, the first PPTP message is sent to the second server; and the Hash calculation is performed on the IP address of the client-side extracted from the first GRE message to obtain an IP address same as the IP address of the second server obtained by calculating according to the first PPTP message, and the first PPTP message and the encapsulated first GRE message are sent to the same second server.

[0011] According to an embodiment of the present disclosure, the second server in the second server cluster is obtained

by screening through GRE message interactive communication with a preset GRE protocol simulation test server.

[0012] According to an embodiment of the present disclosure, the method for PPTP VPN based access acceleration further includes: receiving a second PPTP message and an encapsulated second GRE message from the VPN server; de-encapsulating the encapsulated second GRE message based on the first network communication protocol to obtain a second GRE message; extracting source addresses in the second PPTP message and the second GRE message, and changing the source addresses in the second PPTP message and the second GRE message to the IP address of the client-side; and sending the second PPTP message and the second GRE message, of which the source addresses are changed to the IP address of the client-side, to the client-side.

[0013] The present disclosure also provides a PPTP VPN based access acceleration apparatus, wherein a PPTP VPN system includes a client-side, a first server, a VPN server, and a second server cluster supporting a GRE protocol connected between the first server and the VPN server, and the second sever cluster is an acceleration system. The PPTP VPN based access acceleration apparatus comprises: a first receive unit configured to receive a first PPTP message and a first GRE message from a same client-side and a second PPTP message, and to an encapsulated second GRE message from the VPN server that are fed back via the second server; a first encapsulation/de-encapsulation unit configured, based on the first network communication protocol, to encapsulate the first GRE message and de-encapsulate the encapsulated second GRE message; a first extraction processing unit configured to extract source addresses in the second PPTP message and a second GRE message, and change the source addresses in the second PPTP message and the second GRE message to an IP address of the client-side; and a first transmit unit configured to send the first PPTP message and an encapsulated first GRE message to the second server, and send the second PPTP message and the second GRE message, of which the source addresses are changed to the IP address of the client-side, to the client-side.

[0014] According to an embodiment of the present disclosure, the PPTP VPN based access acceleration apparatus according further includes: a first analysis processing unit configured to: extract the IP address of the client-side from the first PPTP message and the first GRE message, respectively; perform Hash calculation on the IP address of the client-side extracted from the first PPTP message to obtain an IP address of the second server; perform the Hash calculation on the IP address of the client-side extracted from the first GRE message to obtain an IP address same as the IP address of the second server obtained by calculating according to the first PPTP message; and the first transmit unit configured, according to analysis processing result of the first analysis processing unit, to send the first PPTP message and the encapsulated first GRE message to the same second server.

[0015] According to an embodiment of the present disclosure, the first network communication protocol is a network communication protocol that supports the transmission of data packets between the first server and a second server in the process of network communication.

[0016] the present disclosure also provides a method for PPTP VPN based access acceleration, wherein a PPTP VPN system includes a client-side, a first server, a VPN server, and a second server cluster supporting a GRE protocol connected between the first server and the VPN server, and the second sever cluster is an acceleration system. The method for PPTP VPN based access acceleration comprises: receiving a first PPTP message and an encapsulated first GRE message from a same client-side; de-encapsulating the encapsulated first GRE message according to a first internet communication protocol to obtain a first GRE message; extracting destination addresses and source addresses in the first PPTP message and the first GRE message, wherein the destination addresses are an IP address of the VPN server, and the source addresses are an IP address of the client-side; changing the source addresses of the first PPTP message and the first GRE message to an IP address of the second server; wherein the second server is arranged on the route between the first server and the VPN server and is closest to the VPN server; and according to the destination addresses, sending the first PPTP message and the first GRE message, whose source addresses are changed to the IP address of the second server, to the VPN server.

[0017] According to an embodiment of the present disclosure, the first network communication protocol is a network communication protocol that supports the transmission of data packets between the first server and a second server in the process of network communication.

[0018] According to an embodiment of the present disclosure, the first sever is connected with the client-side or the first server is a virtual server arranged on the client-side.

[0019] According to an embodiment of the present disclosure, the second server in the second server cluster is obtained by screening through GRE message interactive communication with a preset GRE protocol simulation test server.

[0020] According to an embodiment of the present disclosure, the method for PPTP VPN based access acceleration according further includes: receiving a second PPTP message and a second GRE message from the VPN server; encapsulating the second GRE message based on the first network communication protocol; and sending the second PPTP message and an encapsulated second GRE message to the first server.

[0021] The present disclosure also provides a PPTP VPN based access acceleration apparatus, wherein a PPTP VPN system includes a client-side, a first server, a VPN server, and a second server cluster supporting a GRE protocol connected between the first server and the VPN server, and the second sever cluster is an acceleration system. The

PPTP VPN based access acceleration apparatus comprises: a second receive unit configured to receive a first PPTP message and an encapsulated first GRE message from the first server, and a second PPTP message and a second GRE message from the VPN server; a second encapsulation/de-encapsulation unit configured, based on the first network communication protocol, to encapsulate the first GRE message and de-encapsulate an encapsulated second GRE message; a second extraction processing unit configured to extract source addresses in the first PPTP message and a first GRE message, and change the source addresses in the first PPTP message and the first GRE message to an IP address of the second server, wherein the extracted IP addresses are an IP address of the client-side; and a second transmit unit configured to send the first PPTP message and the first GRE message, of which the source addresses are changed to the IP address of the second server, to the VPN server, and send the second PPTP message and an encapsulated second GRE message to the first server.

[0022] According to an embodiment of the present disclosure, the first network communication protocol is a network communication protocol that supports the transmission of data packets between the first server and a second server in the process of network communication.

[0023] The present disclosure also provides a device. The device utilizes the above-mentioned PPTP VPN based access acceleration apparatus.

[0024] As described above, the method, apparatus, and device for PPTP VPN provided by the present disclosure has the following beneficial effects.

[0025] Based on setting the GRE protocol simulation test server, the server cluster (the plurality of VPN servers that are connected between the first server and the VPN server) is detected to select the second servers that support the GRE protocol, thereby forming the second server cluster that support the GRE protocol.

[0026] The HASH algorithm is used to calculate the IP address of the same client-side so that the PPTP messages and GRE messages sent by the same client are transmitted over the same path. Therefore, the acceleration system can support the PPTP VPN access.

[0027] In order to ensure the stability of data transmission, GRE messages are encapsulated at the first server based on the TCP protocol. The quality of user access is improved.

[0028] After the second server cluster acceleration, the speed at which the user accesses the source station is greatly accelerated.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029]

FIG. 1 is a schematic diagram of a conventional agent system;

FIG. 2 is a schematic diagram of a PPTP VPN acceleration system according to embodiments of the present disclosure;

FIG. 3 is a schematic diagram of a PPTP VPN system for determining whether a second server in a server cluster supports a GRE protocol according to embodiments of the present disclosure;

FIG. 4 is a flow chart of a method for PPTP VPN based access acceleration according to an embodiment of the present disclosure;

FIG. 5 is a schematic diagram of a common GRE message format;

FIG. 6 is a schematic diagram of a format of a GRE message encapsulated using TCP protocol, according to the method for PPTP VPN based access acceleration disclosed in embodiments of the present disclosure;

FIG. 7 is a flow chart of a method for PPTP VPN based access acceleration according to another embodiment of the present disclosure;

FIG. 8 is a flow chart of a method for PPTP VPN based access acceleration according to another embodiment of the present disclosure;

FIG. 9 is a flow chart of a method for PPTP VPN based access acceleration according to another embodiment of the present disclosure;

FIG. 10 is a schematic diagram of a PPTP VPN based access acceleration apparatus according to an embodiment

of the present disclosure; and

FIG. 11 is a schematic diagram of a PPTP VPN based access acceleration apparatus according to another embodiment of the present disclosure.

Description of Components and Labels

[0030]

110	**A** server
120	**B** server
210	client-side
220	first server
230	second server cluster
231, 232	second servers
240	VPN server
310	GRE protocol simulation test server
S11~S12, S21~S25, S31~S33, S41~S44	steps
500	PPTP VPN based access acceleration apparatus
510	first receive unit
520	first encapsulation/de-encapsulation unit
530	first extraction processing unit
540	first analysis processing unit
550	first transmit unit
600	PPTP VPN based access acceleration apparatus
610	second receive unit
620	second encapsulation/de-encapsulation unit
630	second extraction processing unit
640	second transmit unit

DETAILED DESCRIPTION

[0031] Hereinafter, implementation of the present disclosure will be described using specific embodiments. Other advantages and effects of the present disclosure will be apparent to a person skilled in the art from what is disclosed in this specification. The present disclosure may also be implemented or applied by other different embodiments. The details in the specification may also be modified or altered according to different perspectives and applications, without departing from the spirit of the present invention. It should be noted that, in the absence of any conflict, the following embodiments and the features of the embodiments may be combined with each other.

[0032] With Reference to the attached drawings, it should be noted that the drawings provided in the following embodiments merely illustrate the basic idea of the present invention in a schematic manner. Thus, the drawings merely show the components related to the present invention, rather than in accordance with the number, shape, and size of the components in actual implementation. In actual implementation, the type, quantity, and proportion of each component can be randomly changed, and the type of component layout may also be more complex.

[0033] The present disclosure provides a method, apparatus, and device for PPTP VPN based access acceleration. The PPTP VPN system as shown in FIG. 2 includes a client-side 210, a first server 220, a second server cluster 230, and a VPN server 240. Via the PPTP VPN system, a user can establish a virtual data link between the client-side 210 and the VPN server 240.

[0034] The first server 220 may be a virtual server in the form of a software installed in the client-side 210 or a router, a gateway, and/or a switch connected to the client-side 210 over internet. As shown in FIG. 2, the first server 220 of the present embodiment is a router that is arranged at the client-side 210, and is connected to the client-side 210 via a network.

[0035] The second server cluster 230 includes a plurality of second servers that support the GRE protocol and the plurality of second servers are interconnected to each other.

[0036] In conventional VPN agent systems, not all servers can support the GRE protocol. There may be hundreds or thousands of servers connected between the first server 220 and the VPN server 240. However, the back-to-the-source server must support the GRE protocol. Moreover, the number of servers connected between the first server 220 and the VPN server 240 is extremely large. It is unrealistic to select out the servers that support the GRE protocol manually with manpower. Therefore, the present disclosure makes an intelligent decision on the plurality of servers connected between the first server 220 and the VPN server 240, from which second servers that support the GRE protocol are

selected to form the second server cluster 230. As shown in FIG. 3, a GRE protocol simulation test server 310 (the GRE protocol simulation test server determines whether the GRE protocol transmission is supported manually with manpower) that supports the GRE protocol is arranged outside the PPTP VPN system. The GRE simulation server is connected to the server cluster (a plurality of servers connected between the first server 220 and the VPN server) via the Internet. In addition, in order to ensure the accuracy of the decision, one GRE protocol simulation test server 310 is arranged on each carrier line.

[0037] When performing the selection of the second servers that support the GRE protocol, simulating an interactive communication based on the GRE messages between the GRE protocol simulation test server 310 and the servers (the plurality of servers connected between the first server 220 and the VPN server) is performed, and the IP address of the GRE protocol simulation test server 310 is arranged on all the servers connected between the first server 220 and the VPN server. When the server in the server cluster (the plurality of servers connected between the first server 220 and the VPN server 240) initiates for the first time, the first-initiated server starts a simulated GRE request response to the GRE protocol simulation test server 310. If the server can successfully complete the request response, then the server is determined to support the GRE protocol. That is, the server is a second server. Based on the above method, all the servers (i.e., second servers) that support the GRE protocol can be selected from the server cluster to further form the second server cluster 230 as an acceleration system.

[0038] The first server 220 is connected to one or more second servers in the second server cluster 230. The VPN server 240 is also connected to one or more second servers in the second server cluster 230.

[0039] Furthermore, the PPTP VPN system is based on PPTP VPN, which can use both the GRE and PPTP protocols at the same time. The source IP addresses of both protocols are the same.

The First Embodiment

[0040] When the client-side 210 sends a request for a first PPTP message and a first GRE message, on the first server 220, the first PPTP message and the first GRE message are in accordance with the steps shown in FIG. 4 for access acceleration based on the PPTP VPN.

[0041] Step S11, receiving the first PPTP message and the first GRE message from the same client-side 210.

[0042] The first PPTP message sent out by the client-side 210 is a link request of the PPTP, and the first GRE message is a GRE transmission request.

[0043] After receiving the messages from the client-side 210, the received messages are distinguished based on the PPTP and GRE protocols to obtain the first PPTP message and the first GRE message.

[0044] Step S12, for the first PPTP message, the first PPTP message is sent to the second server. For the first GRE message, the first GRE message is encapsulated based on a first network communication protocol and the encapsulated first GRE message is sent to the second server which receives the first PPTP message.

[0045] For the first PPTP message, the IP address of the client-side 210 is extracted and the Hash calculation is performed on the IP address of the client-side 210 to acquire the IP address of the second server, and the first PPTP message is sent to the second server according to the IP address of the second server. In the present embodiment, the second server that receives the first PPTP message is the second server 231. That is, the IP address obtained by the Hash calculation is the IP address of the second server 231.

[0046] For the first GRE message, two parts are processed:

[0047] First, the first GRE message is encapsulated based on the first network communication protocol.

[0048] The GRE protocol is a common routing encapsulation protocol, which can encapsulate packages of certain network protocols so that the encapsulated packages can be transmitted over another network layer protocol. The GRE protocol lacks of encryption mechanism, and has no standard control protocol to ensure the stability and reliability of transmission. That is, if the transmission between two servers directly uses the GRE protocol, data packet loss during transmission cannot be guaranteed, which will seriously affect the transmission efficiency and transmission quality. Moreover, in the PPTP VPN system, there is no guarantee that GRE messages can be transmitted on the line between two servers.

[0049] Accordingly, the present embodiment performs re-encapsulation of the first GRE message based on the first network communication protocol. The first network communication protocol is a network communication protocol that supports the transmission of data packets between the first server and the second server in the process of network communication. The first network communication protocol includes, but is not limited to, TCP protocol, UDP protocol, and so on. In the present embodiment, the first network communication protocol encapsulates the first GRE message by using the TCP protocol having high reliability and strong versatility. Specifically, the format of the first GRE message is shown in FIG. 5, which includes an IP header, a GRE header, and the GRE transmission content. A TCP header is added between the IP header and the GRE header of the original first GRE message. The format of the encapsulated first GRE message is shown in FIG. 6.

[0050] Second, the encapsulated first GRE message is sent to the second server that receives the first PPTP message.

[0051] The IP address of the client-side 210 is extracted based on the first GRE message and the Hash calculation is performed on the IP address of the client-side 210 to obtain an IP address. With the same IP address of the client-side 210, thus, the IP address obtained by the Hash calculation is the same as the IP address of the second server obtained by calculating according to the first PPTP message, which is the IP address of the second server 231. The encapsulated first GRE message is transmitted to the second server 231 according to the IP address acquired by Hash calculation. Thus, the first PPTP message and the encapsulated first GRE message are sent to the same second server 231.

[0052] Since the first PPTP message and the encapsulated first GRE message are sent to the same second server 231, it is further ensured that the PPTP protocol and the GRE protocol use the same IP for back-to-the-source.

[0053] Moreover, the second server 231 may be a transmission ingress point into which the messages (the first PPTP message and the encapsulated first GRE message) enter the second server cluster 230. Within the second server cluster 230, a route with the lowest back-to-the-source latency is selected for the messages transmission. The route with the lowest back-to-the-source latency refers to based on passing through the second server 231, a route between the first server 220 and the VPN server 240 with the lowest back-to-the-source latency. On the route with the lowest back-to-the-source latency, the second server 232 closest to the VPN server 240 may be the transmission egress point of the messages (the messages sent from the VPN server 240 are different from the messages received from the first server 220) in the second server cluster 230. Eventually the messages are outputted to the VPN server 240.In addition, the determination of the route with the lowest back-to-the-source latency is a very mature routing determination technology, which will not be repeated herein.

[0054] The first server 220 sends the first PPTP message and the encapsulated first GRE message to the second server 231. Starting from the second server 231, the first PPTP message and the encapsulated first GRE message are transmitted in the second server cluster 230 in accordance with the route with the lowest back-to-the-source latency until to the second server 232 closest to the VPN server 240. On the second server 232, the access acceleration based on the PPTP VPN is performed according to the procedures shown in FIG. 7.

[0055] Step S21, receiving the first PPTP message and the encapsulated first GRE message from the first server 220.

[0056] Step S22, based on the first network communication protocol, de-encapsulating the encapsulated first GRE message to obtain the first GRE message.

[0057] The transparent transmission based on the GRE protocol is still utilized between the second server 232 and the VPN server 240. Thus, the encapsulated first GRE message received at the second server 232 is de-encapsulated based on the first network communication protocol. Corresponding to the first GRE message on the first server 220, in the present embodiment, the encapsulated first GRE message herein is also de-encapsulated based on the TCP protocol. Specifically, that is, the TCP message header encapsulated in the first GRE message is removed.

[0058] Step 23, the destination addresses and the source addresses in the first PPTP message and the first GRE message are extracted, where the destination addresses are the IP address of the VPN server 240, and the source addresses are the IP address of the client-side 210.

[0059] No matter it is the PPTP message or the GRE message, in which the source address information and destination address information are stored. In the present embodiment, the destination addresses of both the first PPTP message and the first GRE message are the IP address of the VPN server 240, and the source addresses are the IP address of the client-side 210.

[0060] Step S24, the source addresses of the first PPTP message and the first GRE message are changed to the IP address of the second server. The second server is arranged on the route between the first server and the VPN server and is closest to the VPN server.

[0061] Step S25, According to the destination addresses, the first PPTP message and the first GRE message, whose source addresses are changed to the IP address of the second server, are sent to the VPN server.

[0062] The above process is a process of initiating a request from the client-side 210 to the VPN server 240. Accordingly, the VPN server 240 also performs a respond to the request and finally sends the response result back to the client-side 210.

[0063] Because the source addresses of both the first PPTP message and the first GRE message sent to the VPN server 240 are changed to the IP address of the second server, the VPN server 240 send the second PPTP message and the second GRE message, which are fed back for the first PPTP message and the first GRE message, directly back to the second server 232.

[0064] On the second server 232, an access acceleration based on the PPTP VPN is performed according to the procedures shown in FIG. 8.

[0065] Step S31, receiving the second PPTP message and the second GRE message from the VPN server 240.

[0066] Step S32, encapsulating the second GRE message based on the first network communication protocol.

[0067] The data transmission within the second server cluster 230, and between the second server cluster 230 and the first server 220 is based on the PPTP protocol and the first network communication protocol. Therefore, on the second server 232, the second GRE message is also need to encapsulate based on the first network communication protocol. In the present embodiment, the second GRE message is also encapsulated based on the TCP protocol. That

is, the TCP message header is added to the second GRE message.

[0068] Step S33, sending the second PPTP message and the encapsulated second GRE message to the first server 220.

[0069] The transmission process of the second PPTP message and the encapsulated second GRE message in the second server cluster 230 corresponds to the transmission process of the first PPTP message and the encapsulated first GRE message. According to the transmission path of the first PPTP message and the encapsulated first GRE message in the second server cluster 230, the second PPTP message and the encapsulated second GRE message are forwarded back to the second server 231 and then back to the first server 220 via the second server 231.

[0070] On the first server 220, the second PPTP message and the encapsulated second GRE message are in accordance with the steps shown in FIG. 9 for access acceleration based on the PPTP VPN.

[0071] Step S41, receiving the second PPTP message and the encapsulated second GRE message from the VPN server 240.

[0072] The messages received by the first server 220 are not the second PPTP message and the second GRE message directly fed back by the VPN server 240. The received messages are the messages processed by the second server 232. That is, the second PPTP message and the encapsulated second GRE message.

[0073] Step S42, the second encapsulated GRE message is de-encapsulated based on the first network communication protocol to obtain the second GRE message.

[0074] In the present embodiment, the de-encapsulation process is to remove the TCP message header, which is added on the second GRE packet during encapsulating.

[0075] Step S43, extracting the source addresses of the second PPTP message and the second GRE message to change the source addresses of the second PPTP message and the second GRE message to the IP address of the client-side 210, respectively. The source address extracted from the second PPTP message is the IP address of the second server 232, which is arranged on the route with the lowest back-to-the-source latency and is closest to the VPN server.

[0076] Step S44, sending the second PPTP message and the second GRE message, of which the source addresses are changed to the IP address of the client-side 210, to the client-side 210.

[0077] The steps of the above methods are divided merely for the sake of clarity. In implementation, the steps can be combined into one step or certain steps can be broken down into multiple steps. As long as having the same logical relationship, they are within the scope of the protection of this patent. Adding insignificant modifications or introducing insignificant designs to algorithms or processes without changing the core design of the algorithms and processes is within the scope of the patent.

The Second Embodiment

[0078] The present embodiment discloses a PPTP VPN based access acceleration apparatus 500, which is applied to the first server 220, as shown in FIG. 10, and includes the followings.

[0079] A first receive unit 510 configured to receive a first PPTP message and a first GRE message from the same client-side 210, and a second PPTP message and an encapsulated second GRE message from the VPN server 240 that are fed back via the second server.

[0080] A first encapsulation/de-encapsulation unit 520 configured, based on the first network communication protocol, to encapsulate the first GRE message and de-encapsulate the encapsulated second GRE message.

[0081] The first network communication protocol is a network communication protocol that supports the transmission of data packets between the first server and the second server in the process of network communication. The first network communication protocol includes, but is not limited to, TCP protocol, UDP protocol, and so on. In the present embodiment, the TCP protocol having high reliability and strong versatility is utilized. The encapsulation of the first GRE message is to add a TCP header in the first GRE message, and the de-encapsulation of the second GRE message is to remove the TCP header added in the second GRE message.

[0082] A first extraction processing unit 530 configured to extract the source addresses in the second PPTP message and the second GRE message, and change the source addresses in the second PPTP message and the second GRE message to the IP address of the client-side 210. The source address extracted from the second PPTP message is the IP address of the second server 232, which is arranged on the route with the lowest back-to-the-source latency and is closest to the VPN server.

[0083] A first analysis processing unit540 configured to: extract the IP address of the client-side 210 from the first PPTP message and the first GRE message, respectively; perform the Hash calculation on the IP address of the client-side 210 extracted from the first PPTP message to obtain the IP address of the second server 231;and obtain an IP address by performing Hash calculation on the IP address of the client-side 210 extracted from the first GRE message, which is same as the IP address of the second server 231 obtained by calculating according to the first PPTP message.

[0084] A first transmit unit 550 configured, according to the IP address obtained by the analysis processing of the first

analysis processing unit 540, to send the first PPTP message and the encapsulated first GRE message to the second server 231 in the second server cluster 230; and to send the second PPTP message and the second GRE message, of which the source addresses are changed to the IP address of the client-side 210, to the client-side 210.

[0085] In addition, in order to highlight the innovative parts of the present invention, the present embodiment does not introduce units that are not closely related to the technical problem proposed by the present invention, which does not indicate that no other elements exist in the present embodiment.

The Third Embodiment

[0086] The present embodiment discloses a PPTP VPN based access acceleration apparatus 600, which is applied to the second server 232, as shown in FIG. 11, and includes the followings.

[0087] A second receive unit 610 configured to receive a first PPTP message and an encapsulated first GRE message from the first server 220, and a second PPTP message and a second GRE message from the VPN server 240.

[0088] A second encapsulation/de-encapsulation unit 620 configured, based on the first network communication protocol, to encapsulate the first GRE message and de-encapsulate the encapsulated second GRE message.

[0089] The first network communication protocol is a network communication protocol that supports the transmission of data packets between the first server and the second server in the process of network communication. The first network communication protocol includes, but is not limited to, TCP protocol, UDP protocol, and so on. In the present embodiment, the TCP protocol having high reliability and strong versatility is utilized. The encapsulation of the first GRE message is to add a TCP header in the first GRE message, and the de-encapsulation of the second GRE message is to remove the TCP header added in the second GRE message.

[0090] A second extraction processing unit 630 configured to extract the source addresses in the first PPTP message and the first GRE message, and change the source addresses in the first PPTP message and the first GRE message to the IP address of the second server 232. The extracted IP addresses are the IP address of the client-side 210.

[0091] A second transmit unit 640 configured to send the first PPTP message and the first GRE message, of which the source addresses are changed to the IP address of the second server, to the VPN server 240, and send the second PPTP message and the encapsulated second GRE message to the first server 220.

[0092] In addition, in order to highlight the innovative parts of the present invention, the present embodiment does not introduce units that are not closely related to the technical problem proposed by the present invention, which does not indicate that no other elements exist in the present embodiment.

[0093] It is not difficult to find that the first embodiment is a method embodiment corresponding to the second embodiment or the third embodiment, and the first embodiment may be implemented in cooperation with the second embodiment or the third embodiment. The related technical details mentioned in the first embodiment are still valid in the second embodiment or the third embodiment, which, for the sake of reducing repetition, will not be described again in the second embodiment or the third embodiment. Accordingly, the related technical details mentioned in the second embodiment or the third embodiment may also be applied in the first embodiment.

[0094] The method, apparatus, and device for PPTP VPN based access acceleration, which are provided by the present disclosure, utilize the Hash algorithm to calculate the IP address of the same client-side. Therefore, the IP address of the same second server under the minimum consumption can be obtained. In order to ensure the stability of data transmission, the GRE messages are encapsulated on the first server based on the TCP protocol, which improves the quality of user access. In the whole PPTP VPN system, what the user sends from the client is a GRE message, and what the user receives is the same GRE message. The entire process of data transmission is transparent to the user, and through the underlying protocol to further ensure the reliability of transmission, reducing the data packet loss phenomenon. Based on the acceleration of the second server cluster of the present invention, the speed at which the user accesses the source station is greatly accelerated. Therefore, the present invention effectively overcomes the shortcomings of the conventional technologies and has a high degree of industrial use value.

[0095] The above-mentioned embodiments are merely illustrating the principles and effects of the present invention and are not intended to limit the present invention. Any person skilled in the art can modify or alter the above-mentioned embodiments without departing from the spirit and scope of the invention. Therefore, any equivalents, advantages, or alternations within the spirit and principles of the present disclosure performed by the person who have the common knowledge in the technical fields are intended to be encompassed within the claims of the present invention.

Claims

1. A method for PPTP (Point to Point Tunneling Protocol) VPN (virtual private network) based access acceleration, wherein a PPTP VPN system includes a client-side, a first server, a VPN server, and a second server cluster supporting a GRE (Generic Routing Encapsulation) protocol connected between the first server and the VPN server,

and the second sever cluster is an acceleration system, the method for PPTP VPN based access acceleration comprising:

receiving a first PPTP message and a first GRE message from the same client-side;
for the first PPTP message, sending the first PPTP message to a second server; and
for the first GRE message, encapsulating the first GRE message based on a first network communication protocol and sending the encapsulated first GRE message to the second server receiving the first PPTP message.

2. The method for PPTP VPN based access acceleration according to claim 1, wherein the first network communication protocol is a network communication protocol that supports the transmission of data packets between the first server and the second server in the process of network communication.

3. The method for PPTP VPN based access acceleration according to claim 1, wherein the first sever is connected with the client-side or the first server is a virtual server arranged on the client-side.

4. The method for PPTP VPN based access acceleration according to claim 1, wherein:

IP (Internet Protocol) addresses of the client-side are extracted from the first PPTP message and the first GRE message, respectively;
a Hash calculation is performed on the IP address of the client-side extracted from the first PPTP message to obtain an IP address of the second server, and according to the IP address of the second server obtained from the Hash calculation, the first PPTP message is sent to the second server; and
the Hash calculation is performed on the IP address of the client-side extracted from the first GRE message to obtain an IP address same as the IP address of the second server obtained by calculating according to the first PPTP message, and the first PPTP message and the encapsulated first GRE message are sent to the same second server.

5. The method for PPTP VPN based access acceleration according to claim 1, wherein:

the second server cluster includes a plurality of second servers; and
the plurality of second servers in the second server cluster are obtained by screening through GRE message interactive communication with a preset GRE protocol simulation test server.

6. The method for PPTP VPN based access acceleration according to claim 1 further including:

receiving a second PPTP message and an encapsulated second GRE message from the VPN server;
de-encapsulating the encapsulated second GRE message based on the first network communication protocol to obtain a second GRE message;
extracting source addresses in the second PPTP message and the second GRE message, and changing the source addresses in the second PPTP message and the second GRE message to the IP address of the client-side; and
sending the second PPTP message and the second GRE message, of which the source addresses are changed to the IP address of the client-side, to the client-side.

7. A PPTP VPN based access acceleration apparatus, wherein a PPTP VPN system includes a client-side, a first server, a VPN server, and a second server cluster supporting a GRE protocol connected between the first server and the VPN server, and the second sever cluster is an acceleration system, the PPTP VPN based access acceleration apparatus comprising:

a first receive unit configured to receive a first PPTP message and a first GRE message from a same client-side and a second PPTP message, and to an encapsulated second GRE message from the VPN server that are fed back via the second server;
a first encapsulation/de-encapsulation unit configured, based on a first network communication protocol, to encapsulate the first GRE message and de-encapsulate the encapsulated second GRE message;
a first extraction processing unit configured to extract source addresses in the second PPTP message and a second GRE message, and change the source addresses in the second PPTP message and the second GRE message to an IP address of the client-side; and

a first transmit unit configured to send the first PPTP message and an encapsulated first GRE message to the second server, and send the second PPTP message and the second GRE message, of which the source addresses are changed to the IP address of the client-side, to the client-side.

8. The PPTP VPN based access acceleration apparatus according to claim 7 further includes:

a first analysis processing unit configured to extract the IP address of the client-side from the first PPTP message and the first GRE message, respectively; perform Hash calculation on the IP address of the client-side extracted from the first PPTP message to obtain an IP address of the second server; perform the Hash calculation on the IP address of the client-side extracted from the first GRE message to obtain an IP address same as the IP address of the second server obtained by calculating according to the first PPTP message; and
the first transmit unit configured, according to analysis processing result of the first analysis processing unit, to send the first PPTP message and the encapsulated first GRE message to the same second server.

9. The PPTP VPN based access acceleration apparatus according to claim 7, wherein the first network communication protocol is a network communication protocol that supports the transmission of data packets between the first server and the second server in the process of network communication.

10. A method for PPTP VPN based access acceleration, wherein a PPTP VPN system includes a client-side, a first server, a VPN server, and a second server cluster supporting a GRE protocol connected between the first server and the VPN server, and the second sever cluster is an acceleration system, the method for PPTP VPN based access acceleration comprising:

receiving a first PPTP message and an encapsulated first GRE message from the first server;
de-encapsulating the encapsulated first GRE message based on a first internet communication protocol to obtain a first GRE message;
extracting destination addresses and source addresses in the first PPTP message and the first GRE message, wherein the destination addresses are an IP address of the VPN server, and the source addresses are an IP address of the client-side;
changing the source addresses of the first PPTP message and the first GRE message to an IP address of a second server; wherein the second server is arranged on the route between the first server and the VPN server and is closest to the VPN server; and
according to the destination addresses, sending the first PPTP message and the first GRE message, whose source addresses are changed to the IP address of the second server, to the VPN server.

11. The method for PPTP VPN based access acceleration according to claim 10, wherein the first network communication protocol is a network communication protocol that supports the transmission of data packets between the first server and the second server in the process of network communication.

12. The method for PPTP VPN based access acceleration according to claim 10, wherein the first sever is connected with the client-side or the first server is a virtual server arranged on the client-side.

13. The method for PPTP VPN based access acceleration according to claim 10, wherein the second server in the second server cluster is obtained by screening through GRE message interactive communication with a preset GRE protocol simulation test server.

14. The method for PPTP VPN based access acceleration according to claim 10 further including:

receiving a second PPTP message and a second GRE message from the VPN server;
encapsulating the second GRE message based on the first network communication protocol; and
sending the second PPTP message and an encapsulated second GRE message to the first server.

15. A PPTP VPN based access acceleration apparatus, wherein a PPTP VPN system includes a client-side, a first server, a VPN server, and a second server cluster connected between the first server and the VPN server, and the second sever cluster is an acceleration system, the PPTP VPN based access acceleration apparatus comprising:

a second receive unit configured to receive a first PPTP message and an encapsulated first GRE message from the first server, and a second PPTP message and a second GRE message from the VPN server;

a second encapsulation/de-encapsulation unit configured, based on the first network communication protocol, to encapsulate the first GRE message and de-encapsulate an encapsulated second GRE message;
a second extraction processing unit configured to extract source addresses in the first PPTP message and a first GRE message, and change the source addresses in the first PPTP message and the first GRE message to an IP address of the second server, wherein the extracted IP addresses are an IP address of the client-side; and
a second transmit unit configured to send the first PPTP message and the first GRE message, of which the source addresses are changed to the IP address of the second server, to the VPN server, and send the second PPTP message and an encapsulated second GRE message to the first server.

16. The PPTP VPN based access acceleration apparatus according to claim 15, wherein the first network communication protocol is a network communication protocol that supports the transmission of data packets between the first server and the second server in the process of network communication.

17. A device utilizing the PPTP VPN based access acceleration apparatus according to claims 7 or 15.

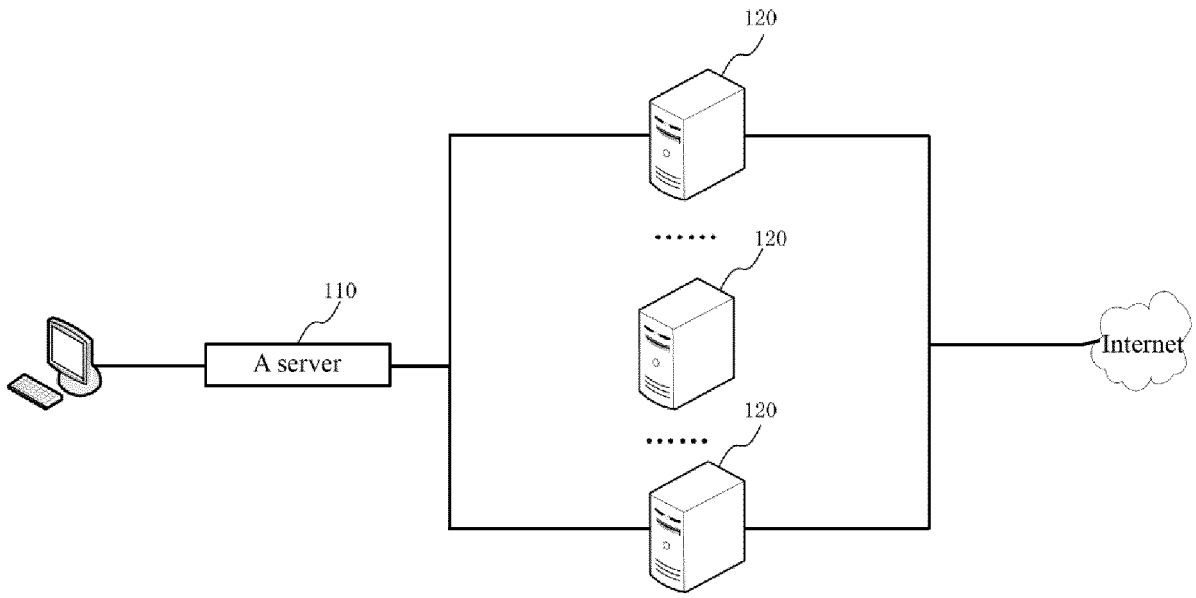
120
120
120
110
A server
Internet

FIG. 1

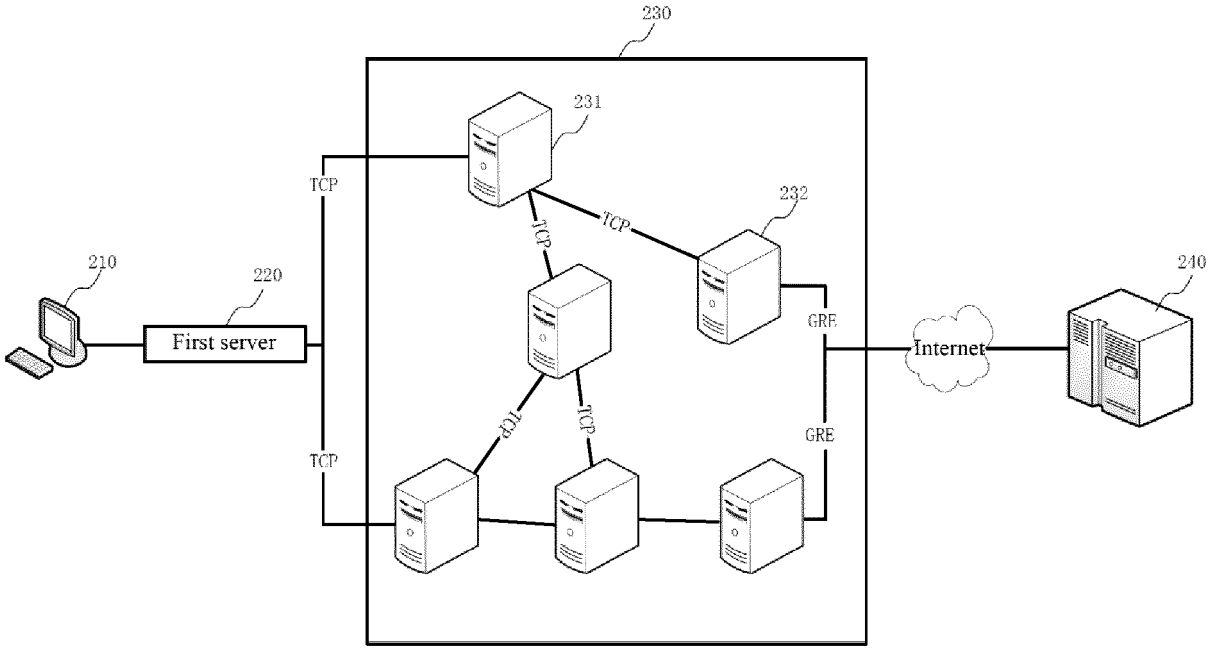
230
231
232
TCP
TCP
TCP
TCP
TCP
TCP
GRE
GRE
210
220
First server
Internet
240

FIG. 2

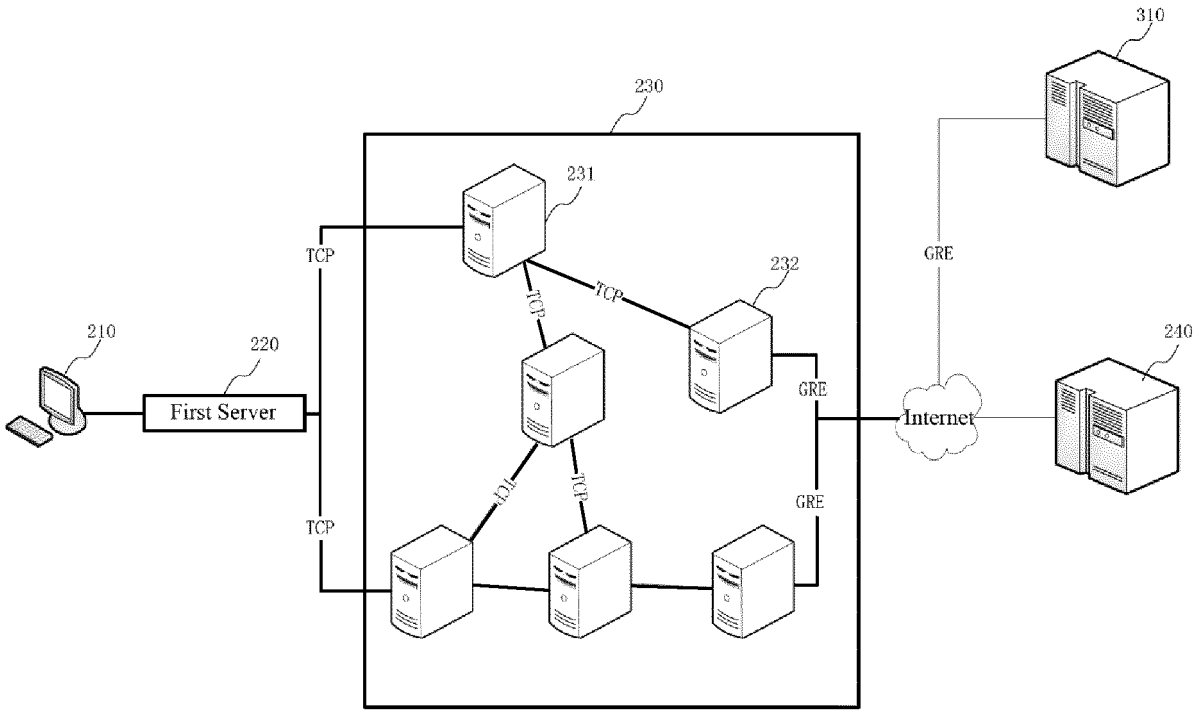
310
230
231
232
TCP
TCP
TCP
TCP
TCP
GRE
GRE
GRE
210
220
First Server
Internet
240

FIG. 3

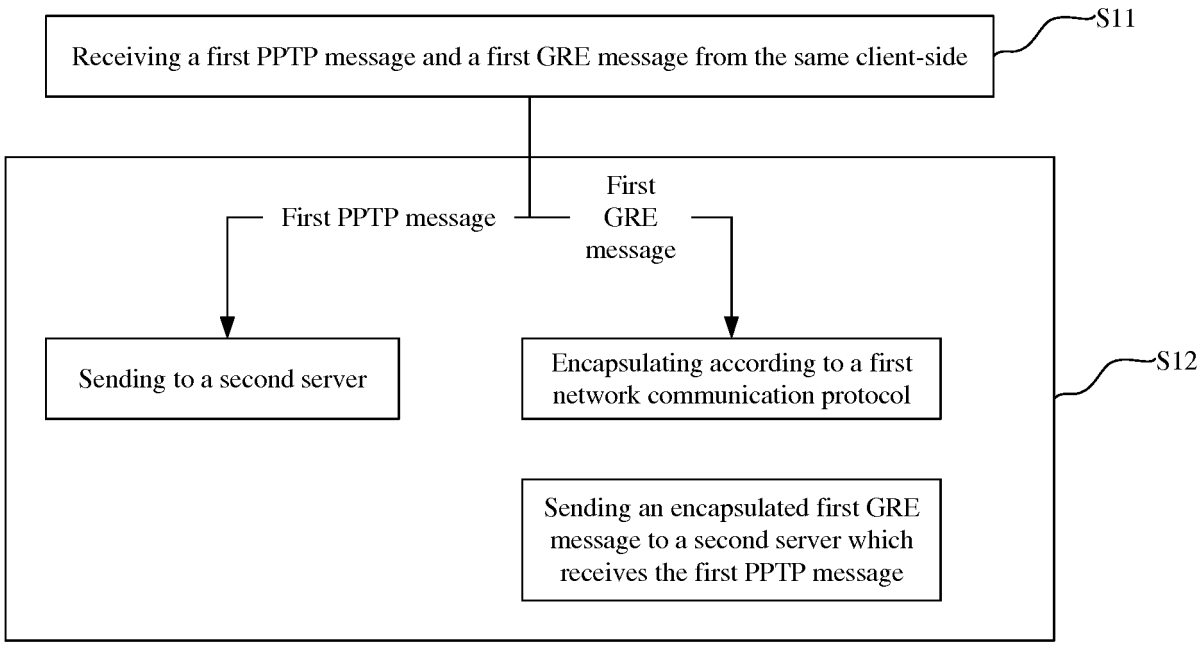
Receiving a first PPTP message and a first GRE message from the same client-side
S11
First PPTP message
First GRE message
Sending to a second server
Encapsulating according to a first network communication protocol
Sending an encapsulated first GRE message to a second server which receives the first PPTP message
S12

FIG. 4

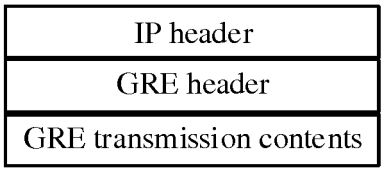

FIG. 5

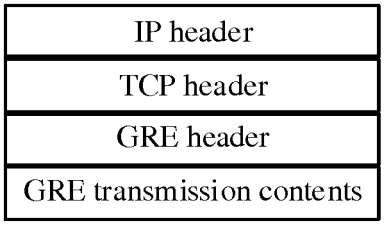

FIG. 6

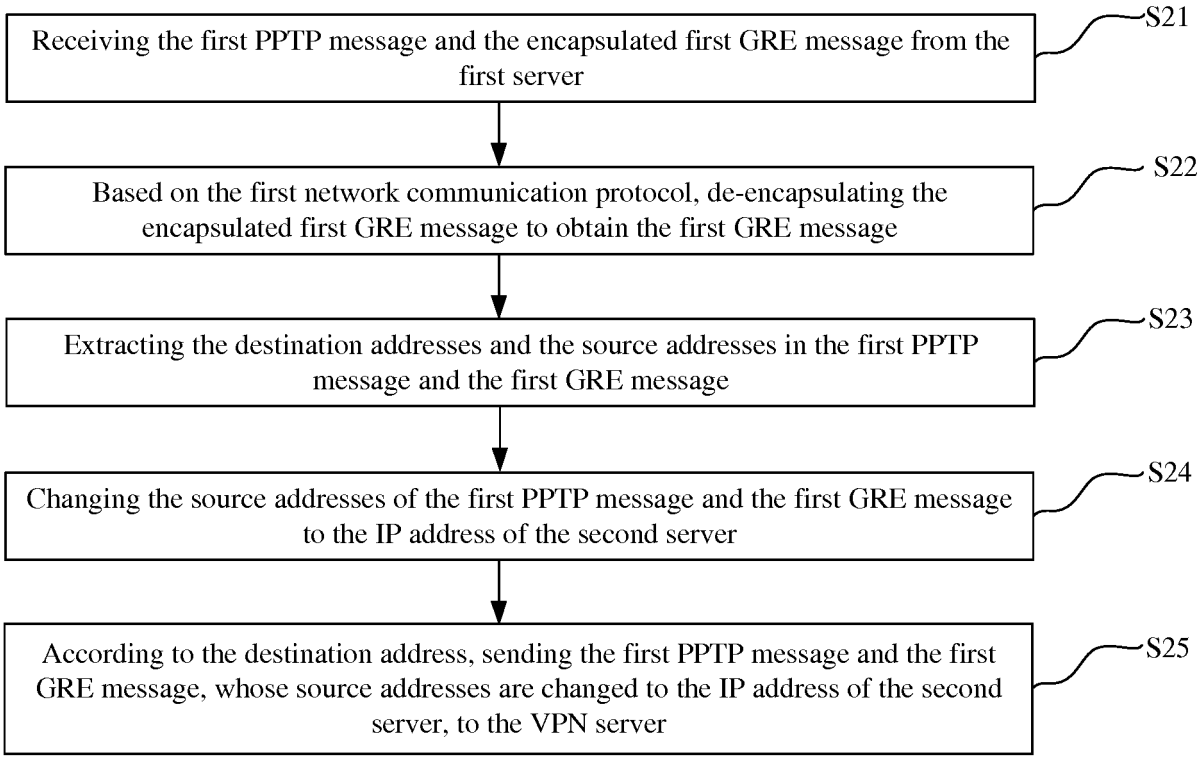

FIG. 7

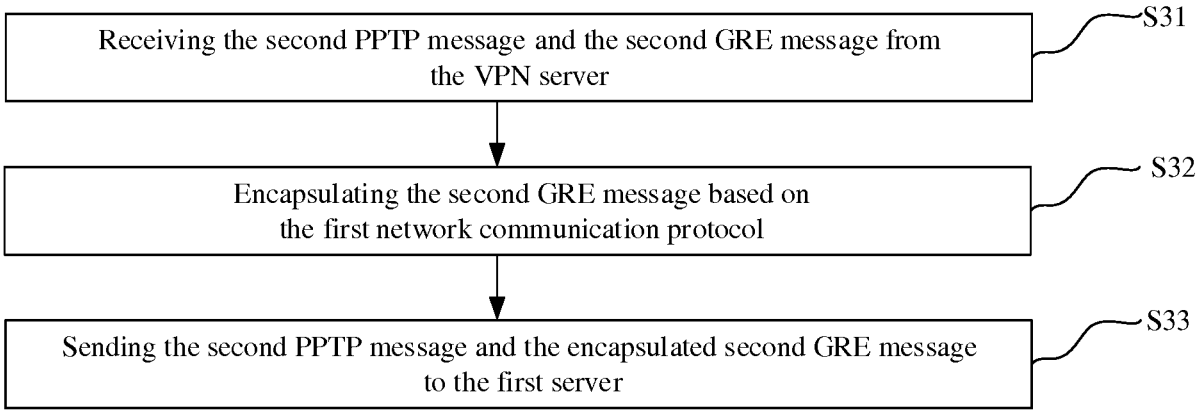
Receiving the second PPTP message and the second GRE message from the VPN server
S31
Encapsulating the second GRE message based on the first network communication protocol
S32
Sending the second PPTP message and the encapsulated second GRE message to the first server
S33

FIG. 8

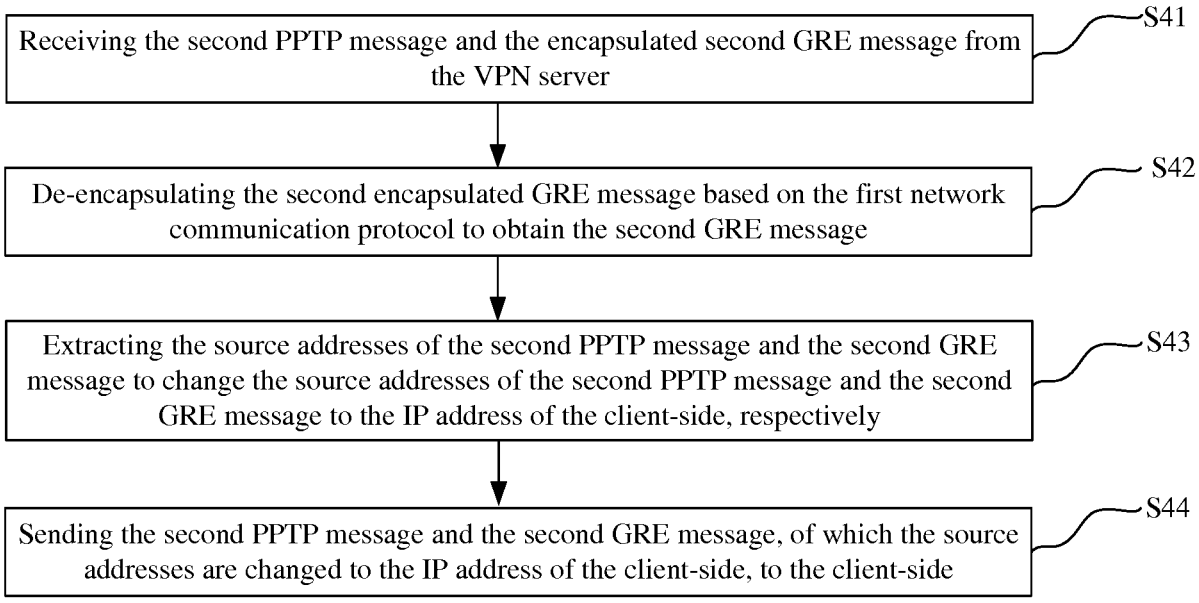
Receiving the second PPTP message and the encapsulated second GRE message from the VPN server
S41
De-encapsulating the second encapsulated GRE message based on the first network communication protocol to obtain the second GRE message
S42
Extracting the source addresses of the second PPTP message and the second GRE message to change the source addresses of the second PPTP message and the second GRE message to the IP address of the client-side, respectively
S43
Sending the second PPTP message and the second GRE message, of which the source addresses are changed to the IP address of the client-side, to the client-side
S44

FIG. 9

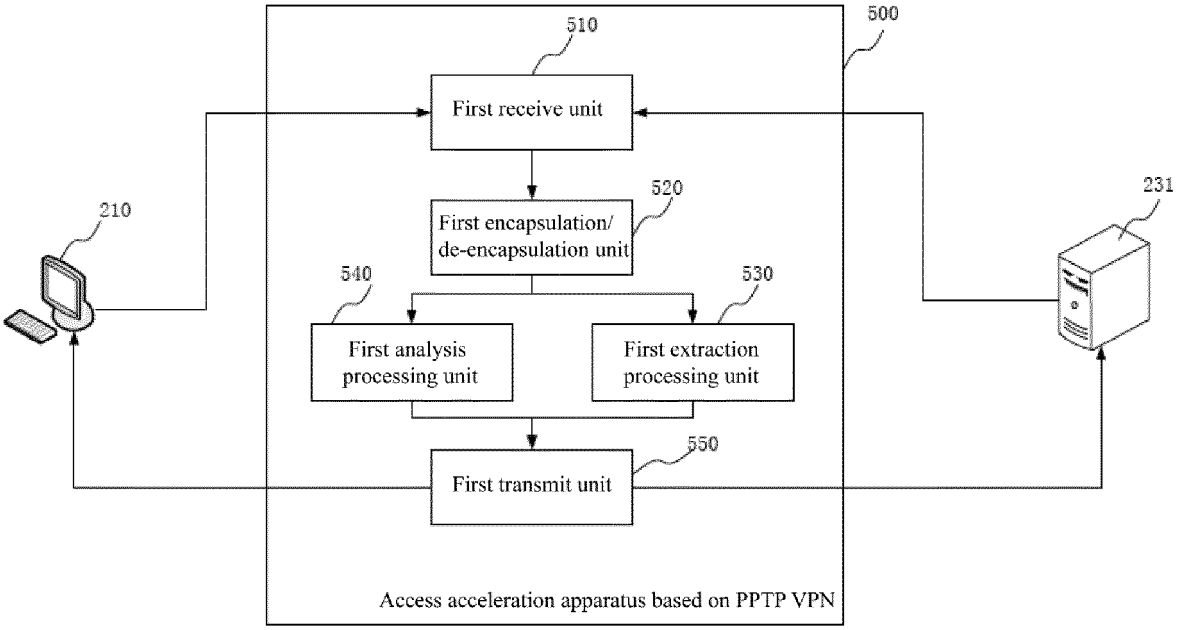
500
510
First receive unit
520
First encapsulation/ de-encapsulation unit
210
231
540
530
First analysis processing unit
First extraction processing unit
550
First transmit unit
Access acceleration apparatus based on PPTP VPN

FIG. 10

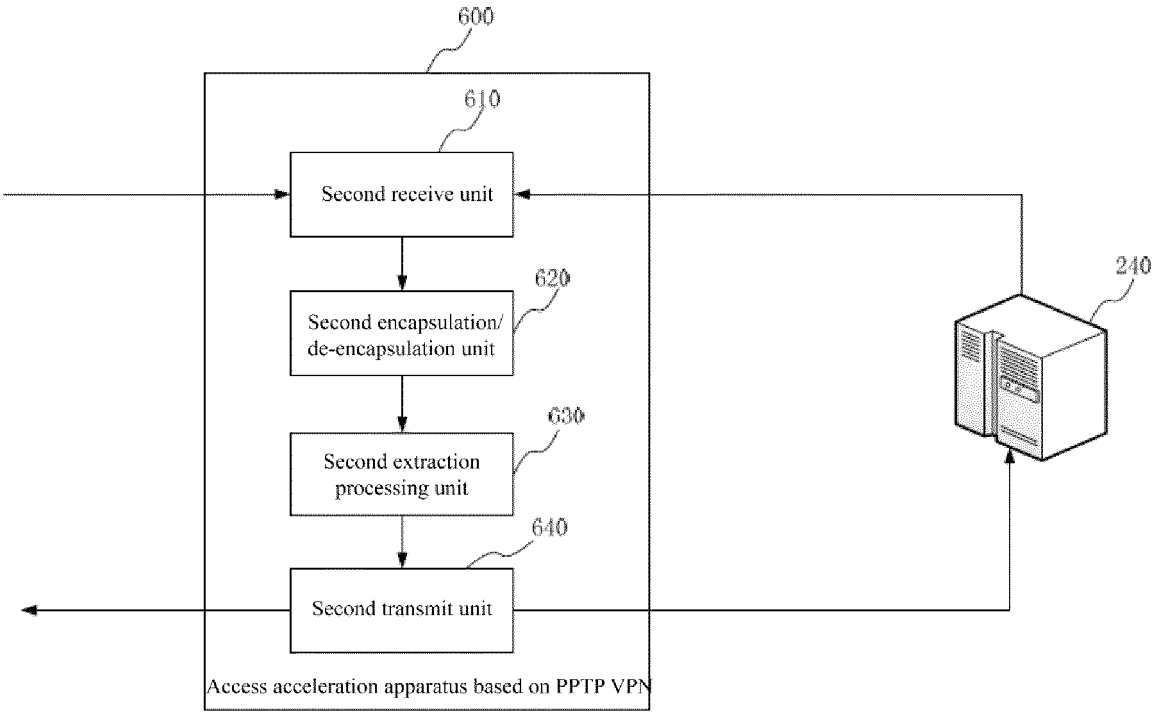
600
610
Second receive unit
620
Second encapsulation/ de-encapsulation unit
240
630
Second extraction processing unit
640
Second transmit unit
Access acceleration apparatus based on PPTP VPN

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/106057

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI; EPODOC; CNPAT; CNKI; IETF: 点对点 2w 隧道, 虚拟 2w 专用网, 服务器, 路由器, 群, 通用 w 路由 w 协议, 封装; PPTP, VPN, server?, router, group, GRE, encapsulat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104935490 A (SHANGHAI DMT INFORMATION NETWORK CO., LTD.), 23 September 2015 (23.09.2015), description, paragraphs [0002]-[0014] and [0038], and figure 1	1-17
A	CN 103391234 A (XIAMEN MEIYA PICO INFORMATION CO., LTD.), 13 November 2013 (13.11.2013), entire document	1-17
A	CN 202957840 U (GOLD SEA COMMUNICATIONS CO., LTD.), 29 May 2013 (29.05.2013), entire document	1-17
A	US 6377571 B1 (3COM CORPORATION), 23 April 2002 (23.04.2002), entire document	1-17
A	HAMZEH, K. et al., "Point-to-Point Tunneling Protocol (PPTP)", RFC2637, 31 July 1999 (31.07.1999), entire document	1-17

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 April 2017	31 May 2017

Name and mailing address of the ISA	Authorized officer
State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	ZUO, Linzi Telephone No. (86-10) 62413364

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/106057

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104935490 A	23 September 2015	None	
CN 103391234 A	13 November 2013	None	
CN 202957840 U	29 May 2013	None	
US 6377571 B1	23 April 2002	None	

Form PCT/ISA/210 (patent family annex) (July 2009)